BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	103 60 210.0
Anmeldetag:	20. Dezember 2003
Anmelder/Inhaber:	ROBERT BOSCH GMBH, 70469 Stuttgart/DE
Bezeichnung:	Netzwerkbrücke
IPC:	H04 L 12/46

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 24. November 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Brosig

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

A 9161
03/00
EDV-L

R. 307466

19.12.03 Sk/Bo

ROBERT BOSCH GMBH, 70442 Stuttgart

Netzwerkbrücke

Stand der Technik

Die Erfindung betrifft eine Netzwerkbrücke, insbesondere zur Kopplung von IEEE1394-Bussen.

Stand der Technik

Netzwerke nach IEEE1394 bestehen gemäß Figur 1 aus einer Anzahl von Knoten K1...Kn im Netzwerk, deren theoretische maximale Anzahl durch die Länge der entsprechenden Knoten-ID auf 63 beschränkt ist. Die Knoten-ID zur Adressierung der einzelnen Knoten hat eine Länge von 6 Bit; die Adresse 0x3F ist als Broadcast-Adresse reserviert. Möchte man mehr als 63 Knoten verbinden, besteht die Möglichkeit, mehrere separate Busse über eine Bus-Brücke zu verbinden. Diese Busse können wiederum einzeln über eine Bus-ID adressiert werden. Die Bus-ID hat eine Länge von 10 Bit, was 1024 Bussen entspricht. Dabei ist die Adresse für „Systemweite Broadcast" reserviert. Theoretisch könnten so 1023 x63 Knoten, also 64.449 Knoten zu einem Netzwerksystem verbunden werden.

Ein serieller Bus nach IEEE1394 unterstützt die Übertragung asynchroner und isochroner Daten. Während der Empfang asynchroner Datenpakte von den empfangenden Knoten quittiert werden muss, um eine sichere Datenübertragung zu gewährleisten, ist für isochrone Daten keine Quittung notwendig. Bus-Brücken zur Kopplung mehrerer Busse müssen die Übertragung beider Datentypen unterstützen. Gleichzeitig müssen sie dafür sorgen, dass bei komplexeren Topologien jedes Datenpaket seinen Empfänger erreichen

kann und dass alle, im Netzwerksystem verbundenen Busse mit einem synchronisierten Takt laufen. Der Draft Standard IEEE1394.1 Version 1.04 spezifiziert die Funktionalität einer solchen High Performance Serial Bus Bridge, speziell für den Einsatz in Netzwerken nach IEEE1394b.

Vorteile der Erfindung

Die Netzwerkbrücke mit Mitteln zur Kontrolle des Inhalts und/oder des Volumens ein- und/oder ausgehender Daten, die durch die Netzwerkbrücke bzw. deren Speicher fließen, wobei die Mittel zur Kontrolle des Inhalts und/oder des Volumens von einer übergeordneten Instanz konfigurierbar und/oder steuerbar ausgebildet sind, ermöglicht den Dateninhalt und/oder das Datenvolumen durch die Netzwerkbrücke zu kontrollieren bzw. zu überwachen.

Die Mittel zur Kontrolle des Inhalts und/oder des Volumens können aus einer Software-Komponente bestehen, die in der Netzwerkbrückenarchitektur auf einfache Weise eingefügt werden kann und eine Gateway- und/oder Firewall-Funktionalität aufweist. Dadurch kann der Inhalt und/oder das Volumen der ein- und ausgehenden Daten, die durch die Netzwerkbrücke bzw. deren Speicher fließen, überwacht werden.

Zeichnungen

Anhand der Zeichnungen werden Ausführungsbeispiele der Erfindung näher erläutert. Es zeigen:

Figur 2 ein Architekturmodell für eine Netzwerkbrücke nach der Erfindung

Figur 3 die Steuerung der Netzwerkbrücken-Gateway-Firewall-Funktionalität,

Figur 4 eine alternative Realisierung.

Beschreibung von Ausführungsbeispielen

Bevor die eigentliche Erfindung beschrieben wird, wird zum besseren Verständnis zuerst die Funktionsweise eines Architekturmodells für eine Netzwerkbrücke gemäß IEEE1394 Draft-Version 1.04 vorgestellt. Die Netzwerkbrücke gemäß Figur 2 ist über ihre Ports P1, P2 ... Pn mit jeweils zwei unabhängigen Netzen N1, N2 verbunden und kann Daten empfangen und senden. Im Allgemeinen wird sie Daten aus einem Netz empfangen und in das andere Netz senden. Die Funktionsblöcke "Port", "Configuration ROM", "PHY", "LINK" und "TRANSACTION" entsprechen denen eines normalen Netzwerk-Knotens nach IEEE1394. Zusätzlich verfügt die Netzwerkbrücke über Routing Maps RM und eine Routing-Einheit RE für jedes der beiden Netze. In den Routing Maps RM werden Informationen über die Topologie und Knoten-Adressen in den jeweiligen Netzen bereitgehalten und über die Routing-Einheit RE können Daten zwischen LINK bzw. TRANSACTION und Speicher F der Netzwerkbrücke NB ausgetauscht werden. Nach IEEE1394.1 besteht der Speicher F aus einer Anzahl einzelner FIFOs, die Daten, welche von einem Bus zum anderen transportiert werden sollen, zwischenspeichern. Die Netzwerkbrücke verfügt außerdem über einen internen Timer T ("Cycle Timer"), mit denen sie in der Lage ist, die Takte in den beiden Bussen zu synchronisieren.

Die Steuerung der Routing-Einheiten RE, wie auch der Funktionsblöcke "Port", "Configuration ROM", "PHY", "LINK" und "TRANSACTION" erfolgt über die Funktionseinheiten "Portal Control" PC.

Der Speicher F der Netzwerkbrücke verfügt erfindungsgemäß über eine Netzwerkbrücken-Gateway-Firewall-Funktionalität BGF über die Inhalt und/oder das Volumen der ein- und ausgehenden Daten, die durch den FIFO-Speicher F fließen, kontrolliert werden. Für isochrone Daten sind die zwei oberen Speicherbereiche reserviert. Für asynchrone Daten sind zwei Anfrage (Request)-Speicherbereiche und zwei Antwort (Response)-Speicherbereiche vorgesehen.

Die Kontrolle des Inhalts und/oder des Volumens erfolgt von der übergeordneten Instanz BGF oder ist fest vorgegeben.

Durch die Überprüfung und Steuerung der Daten sind Zugangskontrollen oder auch diverse Filterfunktionen, z.B. Paketfilter, für den Datenfluss von einem Bussegment über die Netzwerkbrücke zum nächsten Bussegment möglich. Dies ist die Grundlage für eine sichere und geschützte Datenübertragung über die Netzwerkbrücke. Im Einzelnen bietet

die "Bridge-Gateway-Firewall-Funktionalität" Schutz vor ungewollten Verbindungen, wie z.B. Hackerangriffe, oder es wird verhindert, dass vertrauliche Daten unerlaubt über die Netzwerkbrücke ausgetauscht werden. Die Netzwerkbrücken-Gateway-Firewall-Funktionalität kann konfiguriert werden bzw. bekommt die benötigten Informationen über geeignete Software-Schnittstellen von einer übergeordneten Instanz, z.B. einer Software-Schicht mit Management- und Konfigurationsaufgaben. Weiterhin ist es möglich, die Netzwerkbrücken-Gateway-Firewall-Funktionalität jeder einzelnen Netzwerkbrücke individuell zu konfigurieren. Das heißt, jede Netzwerkbrücke ist unabhängig von den anderen in der Lage, keine, eine oder mehrere Funktionen eines Gateways oder einer Firewall auszuführen.

Die Netzwerkbrücken-Gateway-Firewall-Funktionalität kann z.B. aus einer sogenannten Control Unit CU und einer Netzwerkbrücken-Gateway-Firewall-Funktionalität (Modul BGF gemäß Figur 3) bestehen, die es ermöglicht, die Daten (Inhalt und Volumen), die durch den Speicher F der Netzwerkbrücke fließen, zu analysieren und zu manipulieren. Die Analyse der Daten kann auf verschiedenen Ebenen, insbesondere in verschiedenen Schichten des OSI-Referenzmodells erfolgen. Das heißt auf unterster (physikalischer) Ebene können die 1394-Paketinformationen geprüft werden, aber nicht nur der 1394-Header, sondern auch der Inhalt der Nutzdaten kann genau analysiert werden. Somit auch die Daten von höheren Schichten, wie z.B. IP-Daten, bis hoch zu den Daten der Anwendungsschicht und den Nutzerdaten. Der Umfang der möglichen Datenanalyse wird insbesondere skalierbar ausgebildet, denn er steht im Verhältnis mit der dafür benötigten Zeit, die wiederum von der Rechenleistung des Prozessors abhängt. Das heißt, dass es z.B. verschiedene Filterregeln gibt, und diese sind wiederum konfigurierbar. Die Konfiguration dieser Filterregeln bzw. der gesamten Funktionalität der Netzwerkbrücken-Gateway-Fireball kann von einer übergeordneten Softwareschicht aus, z.B. der Management- und Konfigurationsschicht (Konfiguration Layer) BMC, geschehen.

Ein möglicher Zugriff auf die Daten erfolgt zu einem Zeitpunkt (1), wenn die Daten in den Speicher-FIFO (2) geschrieben werden. Dort bleiben sie so lange, bis die Netzwerkbrücken-Gateway-Firewall die Daten bearbeitet hat und sie wieder freigibt (3). Diese Art der Realisierung kann angewendet werden, wenn sich die Datenanalyse der Netzwerkbrücken-Gateway-Firewall-Funktionalität auf den Datenumfang beschränkt, der in dem FIFO zwischengespeichert werden kann. Ein Beispiel hierfür ist die Adressfunktion (Quell- und Zieladresse): Die Netzwerkbrücken-Gateway-Firewall-

Control Unit CU scannt die Datenpakte im FIFO auf bestimmte IP-Adressen, die durch die Konfiguration der Netzwerkbrücken-Gateway-Firewall vorgesehen sind und sperrt die Kommunikation von oder zu diesen bestimmten Adressaten. Ein anderes Beispiel ist das Sperren oder Priorisieren von bestimmten Eingangs- und Ausgangsinterfaces, wie z.B. den jeweiligen PHY-Ports. Ein weiteres Beispiel ist die Protokollfunktion der Netzwerkbrücken-Gateway-Firewall: Mit dieser Funktion kann der gesamte Datenverkehr durch die Netzwerkbrücke protokolliert werden. Das heißt, es werden die Netz- und/oder Knotenadressen der Pakete, die die Netzwerkbrücke passieren, in einer Tabelle oder einem Logfile festgehalten und in gewissen Abständen an einen anderen Funktionsblock wie z.B. das Bridge-Management BMC oder an einen bestimmten Knoten, der die Daten auswählt, übermittelt.

Ein etwas anderer Aufbau zur Realisierung der Netzwerkbrücken-Gateway-Firewall zeigt Figur 4. Dort ist zu erkennen, dass der gesamte Datenfluss durch die Netzwerkbrücke ebenfalls durch die "Bridge-Gateway-Firewall" fließt. Dies ist notwendig, wenn sich die Datenanalyse auf mehrere Pakete ausdehnt und diese nicht gleichzeitig im FIFO gespeichert werden können oder wenn die Analyse der Nutzdaten mehr Zeit in Anspruch nimmt und zusätzliche Buffer (Speicher MM) oder mehr Rechenleistung (Prozessor PR) benötigt werden.

Zur möglichen Kontrolle des Datenvolumens kann z.B. für einen bestimmten Zeitraum, der per Konfiguration von außen, d.h. von irgendeinem bestimmten Knoten im Netzwerk oder der BMC jederzeit festgelegt werden kann, die Netzwerkbrücken-Gateway-Firewall die Übertragung der isochronen Kanäle unterbrechen und bei der Übertragung der asynchronen Kanäle den Datenfluss so zu steuern, dass jedem einzelnen Knoten nur eine bestimmte Anzahl von Datenübertragungen erlaubt wird. Ist die Anzahl erreicht, werden weitere Daten von der Netzwerkbrücken-Gateway-Firewall ignoriert.

Die Interaktion der einzelnen Funktionsblöcke innerhalb der Netzwerkbrücke erfolgt über Schnittstellen, über die Daten gelesen und/oder geschrieben werden können. Über eine solche Schnittstelle kann die Management-Konfigurationsschicht BMC, die in Hardware oder in Software ausgebildet sein kann, statistische Daten, Nutzdaten oder Parameter zum Betrieb der Funktionsblöcke manipulieren. Durch das Sammeln verschiedener Daten ist es der Softwareschicht möglich, Statistiken zum laufenden Betrieb der Netzwerkbrücke in kurzer Zeit zu erstellen. Diese können wiederum dazu genutzt werden, den Betrieb der

Funktionsblöcke zu optimieren, indem z.B. Parameter insbesondere der Funktionsblöcke geändert werden. Als Beispiel soll ein Netzwerk nach IEEE1394 dienen, in dem zeitweise überwiegend isochrone Daten, z.B. Audio- und Video-Steams und zeitweise überwiegend asynchrone Daten übertragen werden. Über statistische Auswertungen kann die Management- und Konfigurationsschicht BMC oder darüber liegende Software-Schichten erkennen, dass der Anteil der asynchronen Daten am Gesamtdatenaufkommen stark zunimmt. Es ist dann möglich, denn flexiblen FIFO-Block F so umzukonfigurieren oder ihm entsprechende Vorgaben für ein automatisches Umkonfigurieren zu machen, dass die Speicherbereiche für isochrone Daten verkleinert und für asynchrone Daten vergrößert werden. Die Netzwerkbrücke kann dadurch schnell auf Änderungen reagieren und muss nicht permanent Speicherbereiche für isochrone und asynchrone Datendurchsätze bereithalten.

19.12.03 Sk/Bo

ROBERT BOSCH GMBH, 70442 Stuttgart

Ansprüche

1. Netzwerkbrücke, insbesondere zur Kopplung von IEEE1394-Bussen, beinhaltend:
- Mitteln (BGF) zur Kontrolle des Inhalts und/oder des Volumens ein- und/oder ausgehender Daten, die durch die Netzwerkbrücke bzw. deren Speicher (F) fließen, wobei die Mittel (BGF) zur Kontrolle des Inhalts und/oder des Volumens von einer übergeordneten Instanz (BMC) konfigurierbar und/oder steuerbar ausgebildet sind oder fest vorgegeben sind.

2. Netzwerkbrücke nach Anspruch 1, dadurch gekennzeichnet, dass die übergeordnete Instanz (BMC) eine Management- und/oder Konfigurationsschicht für die Netzwerkbrücke ist.

3. Netzwerkbrücke nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Mittel (BGF) zur Kontrolle des Inhalts und/oder des Volumens aus einer Softwarekomponente innerhalb der Netzwerkbrücken-Architektur bestehen, die eine Gateway- und/oder Firewall-Funktionalität aufweisen.

4. Netzwerkbrücke nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Umfang der Datenanalyse durch die Mittel (BGF) zur Kontrolle des Inhalts und/oder des Volumens skalierbar ausgebildet ist.

5. Netzwerkbrücke nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Mittel (BGF) zur Kontrolle des Inhalts und/oder des Volumens derart ausgebildet sind, dass neben einer Analyse der Daten auch eine Manipulation derselben durchführbar ist.

6. Netzwerkbrücke nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Analyse der Daten und ggf. deren Manipulation in verschiedenen Schichten eines Schichtenmodells, insbesondere des OSI-Referenzmodells, durchführbar ist.

7. Netzwerkbrücke nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Mittel (BGF) zur Kontrolle des Inhalts und/oder des Volumens ausgebildet sind, Adressen, Eingangs- und Ausgangsinterfaces und/oder Protokollinformationen anhand der Auswertung zu sperren oder zu priorisieren.

8. System, bestehend aus mehreren Netzwerkbrücken nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Mittel (BGF) zur Kontrolle des Inhalts und/oder des Volumens in jeder Netzwerkbrücke individuell konfigurierbar sind, um zu ermöglichen, dass jede Netzwerkbrücke unabhängig von der/den anderen in der Lage ist, keine, eine oder mehrere Funktionen eines Gateways oder einer Firewall auszuführen.

R. 307466

19.12.03 Sk/Bo

ROBERT BOSCH GMBH, 70442 Stuttgart

Netzwerkbrücke

Zusammenfassung

Bei einer Netzwerkbrücke sind Mittel (BGF) zur Kontrolle des Inhalts und/oder Volumens ein- und/oder ausgehender Daten, die durch die Netzwerkbrücke bzw. deren Speicher (F) fließen, vorgesehen. Die Mittel (BGF) können von einer übergeordneten Instanz (BMC) konfigurierbar und/oder steuerbar ausgebildet oder fest vorgegeben sein.

(Figur 2)

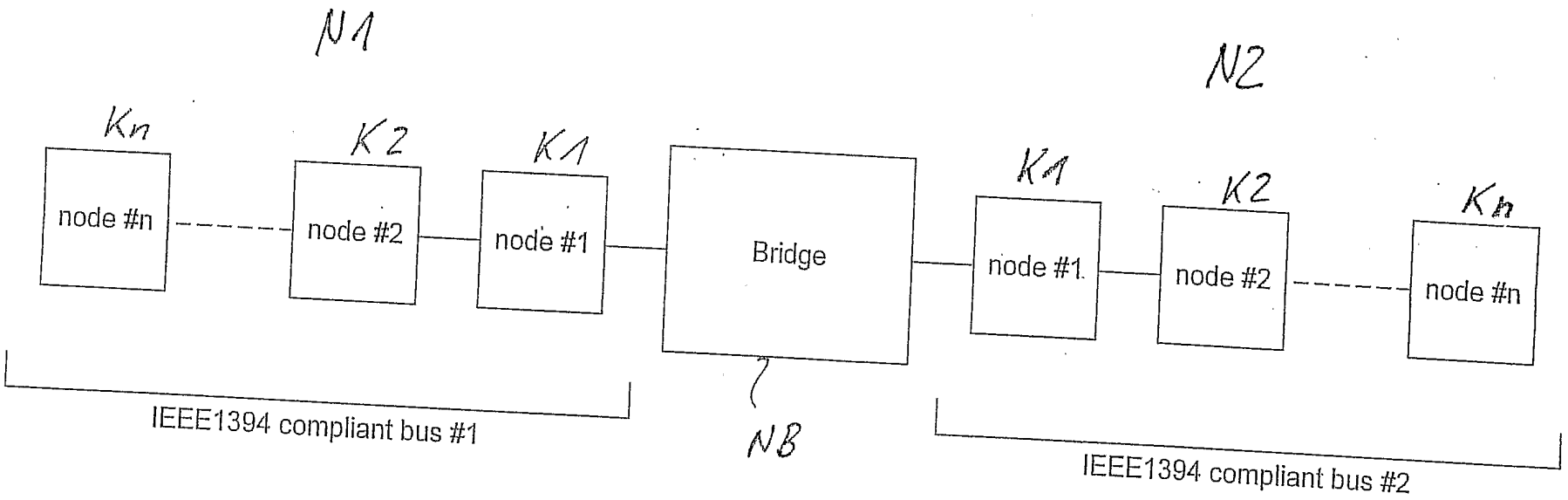
N1
N2
Kn
K2
K1
K1
K2
Kn
node #n
node #2
node #1
Bridge
node #1
node #2
node #n
IEEE1394 compliant bus #1
NB
IEEE1394 compliant bus #2

Fig. 1

214 R.307466

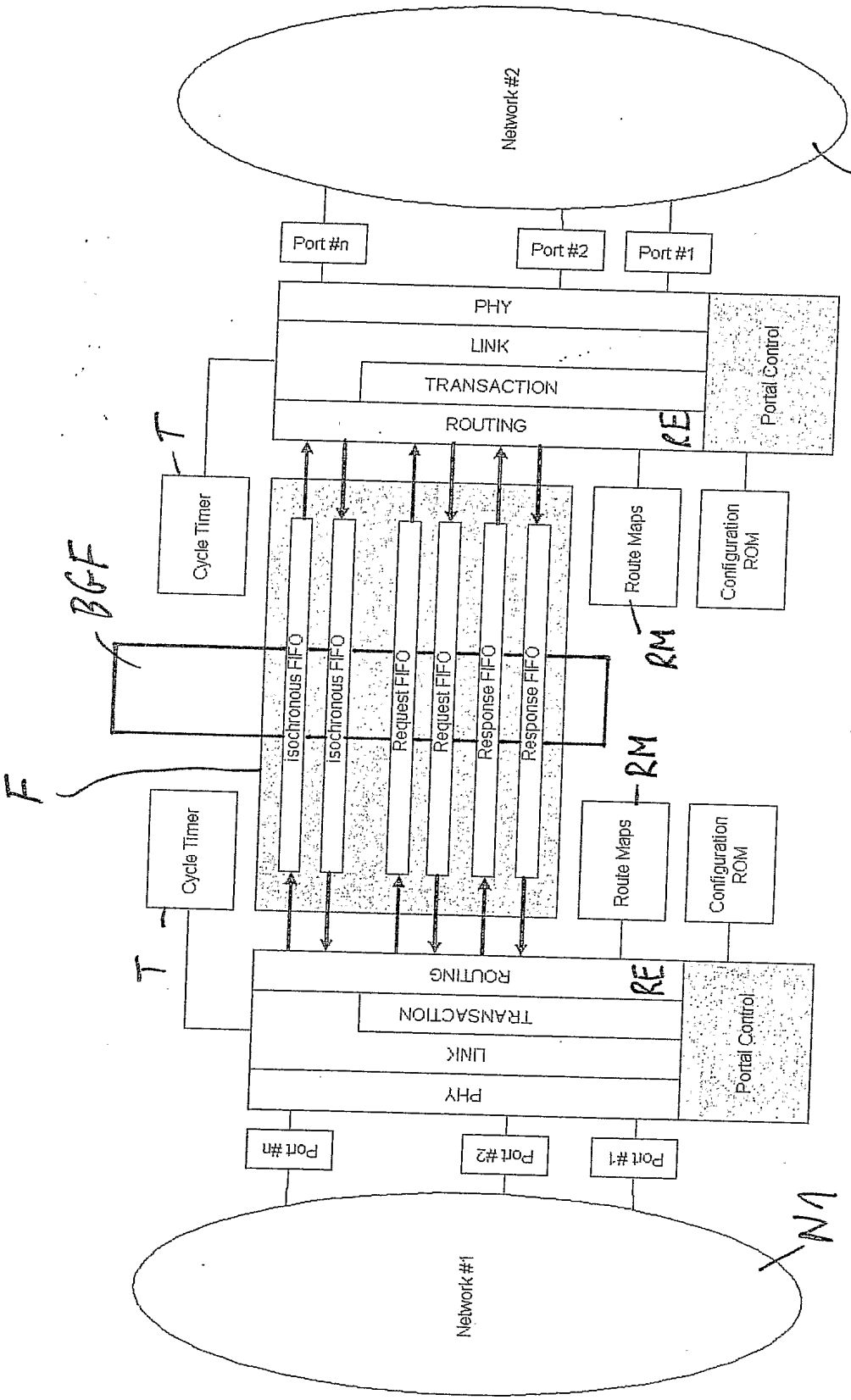

Fig. 2

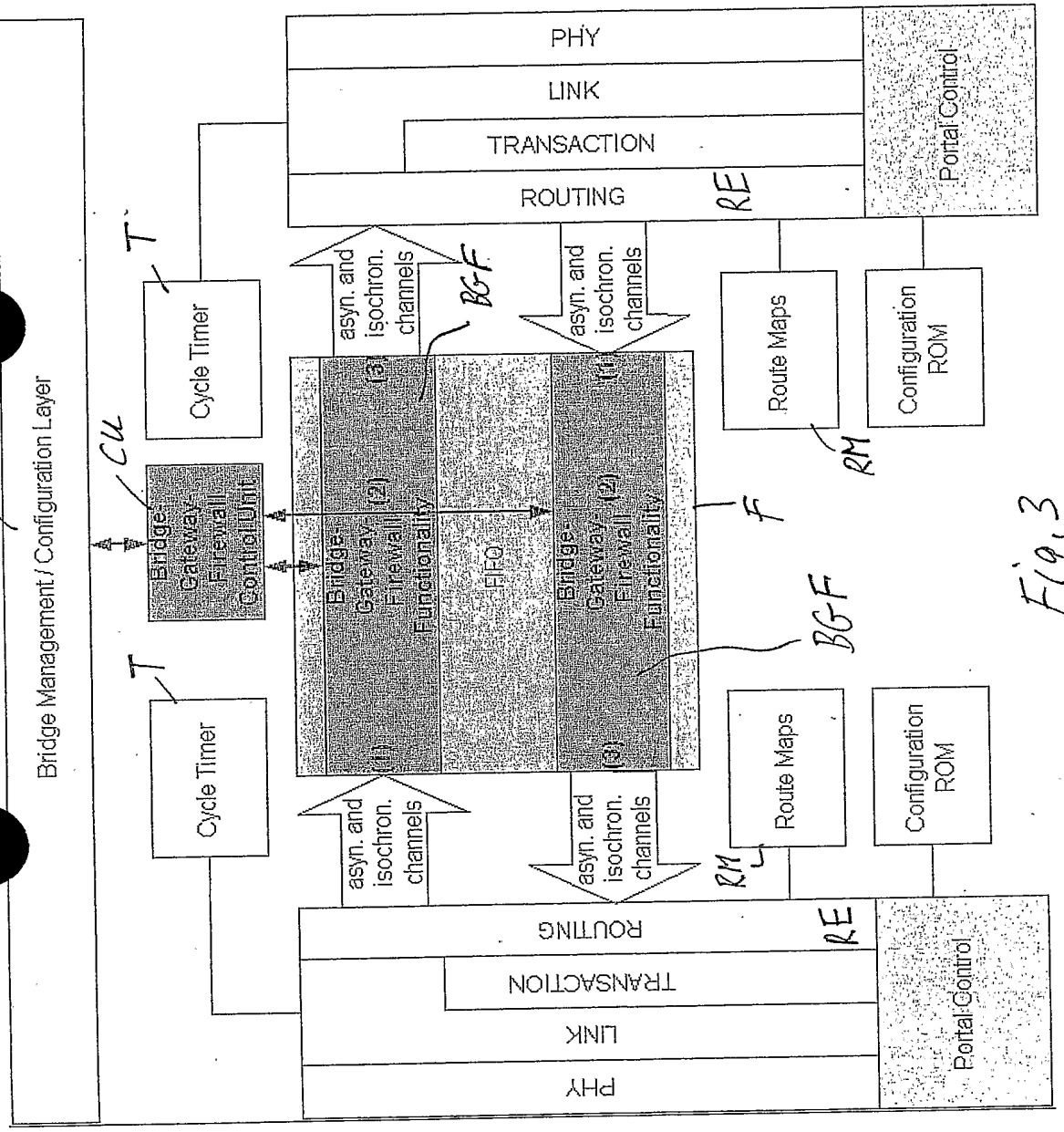
BMC
Bridge Management / Configuration Layer
CU
Bridge Gateway Firewall Control Unit
T
Cycle Timer
T
Cycle Timer
PHY
LINK
TRANSACTION
ROUTING
RE
Portal Control
asyn. and isochron. channels
BGF
asyn. and isochron. channels
Bridge Gateway Firewall Functionality (3)
Bridge Gateway Firewall Functionality (2)
FIFO
Bridge Gateway Firewall Functionality (1)
F
BGF
asyn. and isochron. channels
asyn. and isochron. channels
Route Maps
RM
Configuration ROM
Route Maps
RM
Configuration ROM
RE
Portal Control
ROUTING
TRANSACTION
LINK
PHY

Fig. 3

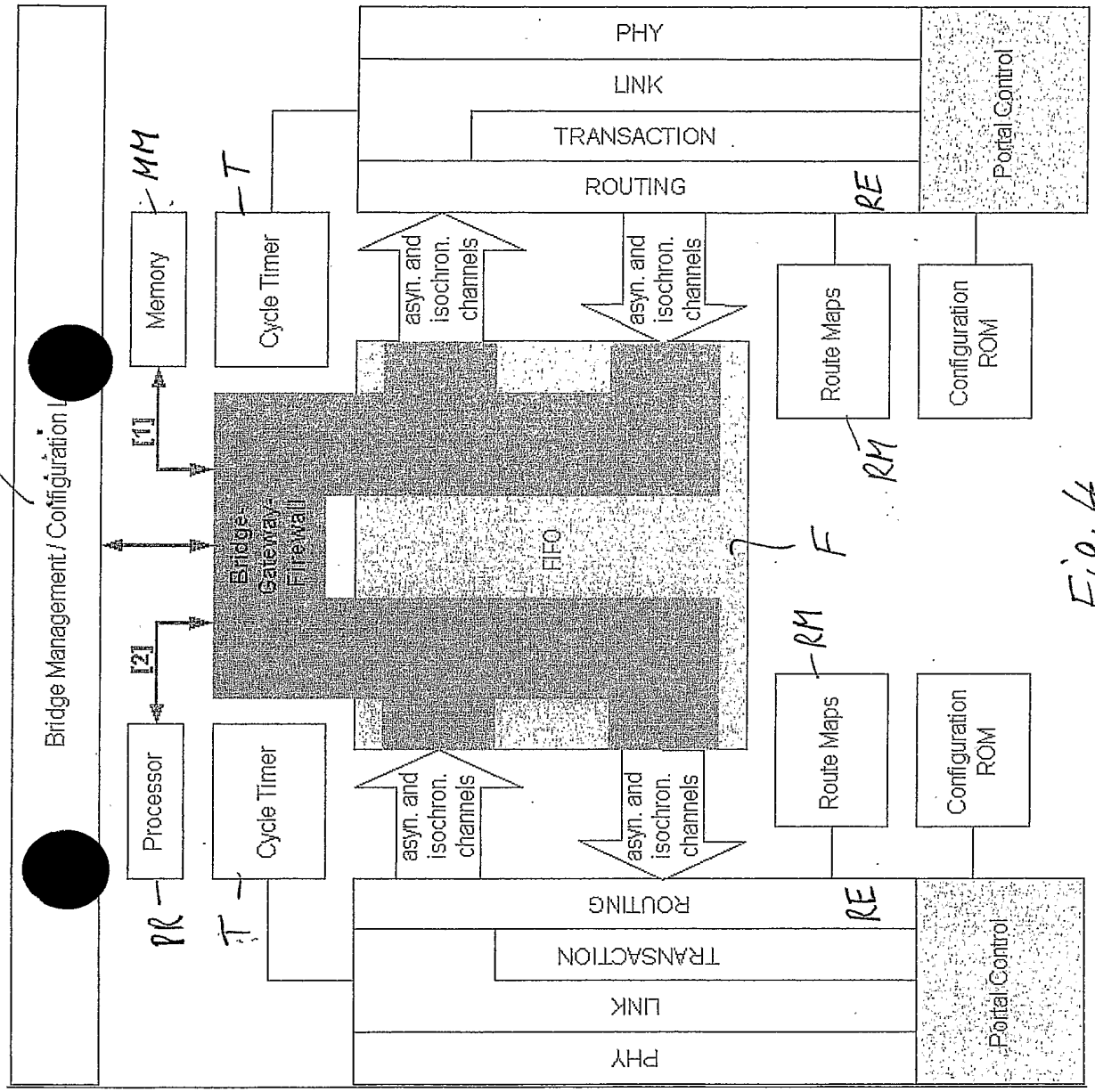
BMC
Bridge Management / Configuration
Memory
MM
Cycle Timer
T
I1
I2
Bridge
Gateway
Firewall
Processor
PR
Cycle Timer
T
PHY
LINK
TRANSACTION
ROUTING
RE
Portal Control
asyn. and isochron. channels
asyn. and isochron. channels
FIFO
F
Route Maps
RM
Configuration ROM
Route Maps
RM
Configuration ROM
ROUTING
RE
TRANSACTION
LINK
PHY
Portal Control
asyn. and isochron. channels
asyn. and isochron. channels

Fig. 4